

Attack Detection Methods for All-Optical Networks

Muriel Médard, Douglas Marquis, and Stephen R. Chinn
Massachusetts Institute of Technology, Lincoln Laboratory
244 Wood Street, Lexington, Massachusetts 02173-9108

Telephone: (781) 981-7650 Fax: (781) 981-4129 Internet: medard@ll.mit.edu, marquis@ll.mit.edu, chinn@ll.mit.edu

Abstract

This paper focuses on theoretical methods for detecting intentional attacks upon the infrastructure of an all-optical network. Applications of existing methods used in traditional networks, as well as discussion of a new method for detecting attacks are presented. Advantages and limitations of both classes of methods are considered.

1. Introduction

All-optical networks (AONs) are a viable technology for future telecommunication and data networks, but their intrinsic security differences with respect to existing electro-optic and electronic networks have only recently received attention [1,2]. This work concentrates on understanding a portion of the security framework for AONs – the study of methods to detect an attack upon an AON. The detection study is broken into two parts: an evaluation of the ability of existing fault detection and diagnostic equipment to detect attacks on AONs, and consideration of a new method for detecting certain attacks. The consideration of all possible attacks is beyond the scope of this paper, but three important attack classes are considered. The results will suggest that while existing methods can detect certain very simple attacks, many other simple attacks (and a large number of advanced attacks) cannot be addressed using current methods. A particularly important reason for the limitations of current methods is *transparency*, a feature of some AONs that allows signals to traverse nodes independently of signal modulation, data rate, and other particular characteristics. The inability of an AON node to interpret the data makes the use of link-by-link forward error correction coding protection mechanisms, which are today's de facto standard, insufficient by themselves for detecting attacks in AONs.

This paper first provides an overview of AON architecture and some results to date. The vulnerabilities of AONs are then reviewed, and the attacks that will be

considered shown. The centerpiece of the paper is then presented, a review of existing diagnostic and attack detection mechanisms, followed by a description of a new method which can more reliably detect attacks in an AON. Finally, a discussion of limitations and unsolved problems is provided.

2. All-Optical Network Overview

An all-optical network (AON) is a network that uses lightwave communication exclusively within the network. More precisely, in an AON all network-to-network interfaces are based on optical transmission, all user-to-network interfaces use optical transmission on the network side of the interface, and all switching and routing within AON network nodes is performed optically. The principal advantage of maintaining an optical network core in comparison to using electro-optic components at nodes or in transmission systems is higher bandwidth: optical bandwidths are generally one thousand fold those of electronic bandwidths, and avoiding optical/electronic/optical conversions therefore promises roughly one thousand times greater data rates than possible with electro-optic networks. Transparency is an optical network feature that allows routing and switching of data within the network without interpretation or regeneration of the individual data streams. While transparency has many desirable features (e.g. terminal upgrades do not require network upgrades), it has important ramifications for security.

Contemporary AONs are still largely in the research arena, though commercial providers are beginning to provide limited AON functions in their networks. The research AONs are divided into two types: wavelength division multiplexed (WDM), which separate multiple channels of traffic each onto its own wavelength, and time-division multiplexed (TDM), which separate multiple channels of traffic each into its own time slot. TDM networks to date [3] have often employed soliton transmission and other features that will likely require further development to reach commercial maturity. Therefore, this paper concentrates on WDM AONs.

Existing AONs are generally architected as circuit-switched networks. Circuit-switched networks are compatible with (1) existing telecommunication installations (long haul), (2) ATM networks, and (3) some multiplexing equipment often used with Internet networks. Fully operational packet-switched AONs have not been implemented in part owing to the lack of a desirable optical memory. AON architecture can generally be divided into optical terminals (which are the user-network interface), network nodes (which switch, route, and sometimes perform mux/demux), and optically amplified fiber optic links. A separate control network (not always all-optical) is usually used for signaling purposes. The switching and routing may be done via mechanical switches, opto-electronic switches, passive optical routers, or splitter/combiners. Common

converting them to electronic signals. One artifact of the amplification is amplified spontaneous emission (ASE) noise, which is added to the output of a signal exiting the amplifier.

Each of these components is susceptible to some form of attack. The description follows in the sections below. It is worth noting that although AONs are not generally commercial products today, each of the above components is commercially available from multiple manufacturers. Some of these components (notably Erbium Doped Fiber Amplifiers) are already deployed in operational telecommunication backbone networks.

The above components have been integrated into testbeds to show the operations and limitations of AONs. AON demonstrations to-date have taken place mostly in

Table 1: Common AON Components

Component	Use	Example
Combiner	Combine optical signals from N fibers to 1 fiber	Star Coupler
Splitter	Split signal from 1 fiber to N fibers	Star Coupler
Demultiplexer	Separate multiple signals on one fiber each onto its own fiber	Waveguide Grating Router
Multiplexer	Combine individual signals from multiple fibers onto one fiber	Waveguide Grating Router
Optical Amplifier	Increases the signal strength (amplitude) of an input signal.	Erbium Doped Fiber Amplifier (EDFA)
Spatial Switch	Let pass or dump a particular signal, or switch it between fibers	LiNbO ₃ Switch
Lasers	Transmit a Signal	Many
Opt Receivers	Receive a Signal	PINFET, Avalanche Photo-diodes
Fiber Cable	Transport	Many

topologies include star, ring, and mesh. Some of the architectures allow a hybrid mixture of topologies.

Although there are a large number of possible architectures, most contemporary WDM AONs are built using a combination of a relatively small set of components. This is very fortunate for this security study, because an understanding of the security properties of each component provides a reasonable foundation for predicting network vulnerabilities and suggesting robust architectures. The most commonly used AON components are shown in Table 1.

A particularly important component is the optical amplifier. Amplifiers are used in both nodes and links of AONs. The amplifier works by using a pump laser and a gain medium to amplify optical signals without

government-funded testbeds or testbeds funded by consortia. In the United States, there are consortia involving academia, industry, and government. In particular, the AON [4], MONET [5], and NTONC [6] consortia have multiple participating organizations and have all developed testbeds. In addition, the European RACE consortium [7], and the Japanese efforts [8] have also developed testbeds. Various testbeds and laboratory experiments have demonstrated aggregate throughputs of over 1 Tbit/s [9]. The traffic carried has consisted of ATM, IP, SONET, Frame Relay, and digitized video.

The remainder of the paper does not consider authentication and cryptographic techniques. There are many interesting cryptographic issues associated with AONs and several methods have been proposed for implementing cryptography in optical communications

[10], [11], [12]. However, in order to determine what the cryptographic needs of an AON might be, it is important to first establish certain characteristics of the network. In particular, it is important to determine how immune the signals are to eavesdropping. Determining the reliability of the network is also crucial, since without satisfactory QoS guarantees, cryptographic issues may be moot. There is a need to address service disruption, which is important to networks used for national security purposes, and increasingly important to broader-use networks such as the Internet [13].

3. Vulnerabilities of All-Optical Networks

This section concentrates on the vulnerabilities of AONs in order to understand and categorize an important and simple set of possible attacks upon these networks. The attacks have specific goals as will be discussed.

3.1. Motivation

The components of AONs discussed in section 2 are each vulnerable to some form of denial of service or eavesdropping-type attack. The attack methods we are most concerned with are jamming – the overpowering of legitimate network signals with attack signals – which can be used to degrade or deny service, and the exploitation of device crosstalk. Device crosstalk exists within most contemporary optical devices, and is the phenomenon where signals from one portion of the optical device leak into another portion of the device. Crosstalk can be used for service denial or eavesdropping attacks. Note that we have not separated signal interception from traffic analysis, instead lumping both under the eavesdropping heading – for this analysis no distinction is necessary. What is necessary is an understanding that detection of attacks in all-optical networks is somewhat different than for electro-optic or electronic networks.

There are many reasons for which, in AONs, (1) attacks must be detected and identified at all points in the network where attacks may occur, and (2) the speed of attack detection should be commensurate with the data transmission rate of the network. The high data rates of AONs have an important consequence for attack detection, essentially because large amounts of data can be affected in a short time. When a fixed duration attack disrupts service, the amount of data affected is linearly proportional to the data rate. Similarly, in an eavesdropping attack, the amount of data compromised is linearly proportional to the data rate. The larger

amounts of data (e.g. number of 'bits in flight') on a particular fiber path for AONs over electro-optic networks means more data is vulnerable to any particular attack than would be in a lower rate network. To illustrate the effect, consider applying to AONs one means of checking for attacks in existing networks – using transport packet verification at the network perimeter. The check on the data may be end-to-end decoding as in some existing electronic networks (e.g. frame relay), or by extension to AONs, be a power test on the received signal as proposed in [14]. In a Tbit/s optical network, perimeter detection of attack combined with a total network path delay on the order of milliseconds will result in Gbits of data having been attacked. Note that, because of transparency, it will not always be possible to place decoding and checking mechanism at several locations throughout an AON to overcome the latency problem.

High AON data rates are not the only reason why identification of attacks should take place at all possible attack locations. An incorrect diagnostic may be given by the network management system. An example is shown in Figure 1. Channel 1 attacks channel 2 via crosstalk (in-band jamming). The output of the switch is a channel with excessive power that causes a gain competition attack on channel 3 at the amplifier. If the amplifier detects the attack of channel 2 on channel 3, but the switch does not detect the attack of channel 1 on channel 2, the network management system may decide to disconnect channel 2. Indeed, the only information available to the network management system is that channel 2 is nefarious at the amplifier, even though channel 1 is the offending channel.

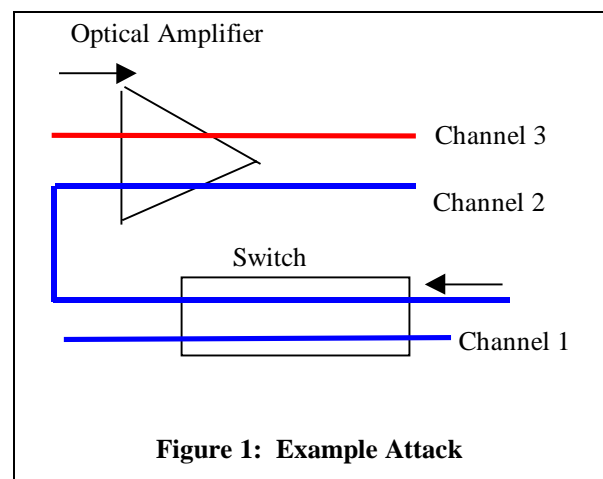


Figure 1: Example Attack

Finally, depending on the algorithms that are used for recovery from attack, it is often necessary to be able to identify an attack and differentiate it from a failure. For

instance, suppose in Figure 1 that channel 2 suffers from a gain competition attack from channel 1 at an amplifier which channels 1 and 2 share. A diagnostic of failure due to insufficient output power from channel 1 might cause the network management system to reroute channels 1 and 2 onto some alternate amplifier(s), which may in turn be attacked by channel 1.

3.2. Attack Types and Methods

Attacks upon a network can be broadly categorized into six areas based on the goal of the attacker: (1) traffic analysis, (2) eavesdropping, (3) data delay, (4) service denial, (5) QoS degradation, (6) spoofing. It is advantageous for the purposes of this work to reduce the scope of the attack methods under consideration as follows: (1) Traffic analysis and eavesdropping have similar characteristics, they may be lumped together; optical networks are somewhat immune to delay attacks owing to the lack of optical memory, and delay attacks are therefore ignored, (2) Spoofing is an attack which may be defended using cryptographic methods alone, and it is therefore not considered here, (3) Service denial is QoS degradation taken to the limit, therefore both can be considered under the label ‘service disruption’.

The resulting attack types are reduced to two: eavesdropping & traffic analysis (hereafter ‘eavesdropping’), and service disruption. A longer attack type list might include areas such as non-repudiation (and others), but such attacks are generally aimed at network protocols, management systems, or operational methods rather than at network infrastructures – infrastructures are our primary concern in this work. Although eavesdropping and traffic analysis generally have vastly different effects upon the legitimate use of the network, this analysis does not require a distinction. At higher network protocol layers, the distinction becomes more important, but at the physical layer, any possible leaking away of legitimate signals is conceptually the same for the purposes of this analysis.

To implement one of the two attack types, an attacker

needs a *method of attack*. To confine the discussion, three particular attacks are considered. They are chosen because they are either very easy to realize, particularly effective against network services, or have an intrinsically different effect than a similar attack against a traditional network. The methods are shown in Table 2.

These methods are not the only methods available to an attacker to realize one of the two attack types. However, these methods are fairly easy to realize using commercially available technology, and could cause major problems in an unsecured AON. Section 3.3 gives examples from each attack method in Table 2.

There are many other possible ways to divide the attack taxonomy problem. For instance, each attack can be categorized by its resources (passive, active); its means of attack (transmission/reception, protocol, control system); the target (specific users or network/subnetwork); the intended effect (traffic analysis or eavesdropping or service disruption); the location of the attack (terminal, node, link, multiple locations), and the attacker’s willingness to be discovered (covert, subtle, overt). All combinations of the above list would yield 576 possible attack domains, not all of which are plausible or will be considered herein.

3.3. Component Vulnerabilities

Each of the components of an AON listed in Table 1 is vulnerable to an attack from Table 2. Three examples summarize the possibilities.

Consider first an *in-band jammer* using a single high-power transmitter that is injected into a link. The attack can destroy a signal on that link — not unlike a traditional network. But in an AON, that attack can degrade signals on that link and on other network links attached to that node. This is due to transparency, which lets signals flow through nodes without regenerating them.

Table 2: AON Attack Methods

Attack Method	Realizes	Means
In-Band Jamming	Service Disruption	An attacker injects a signal designed to reduce the ability of the receiver to interpret correctly the transmitted data
Out-of-Band Jamming	Service Disruption	An attacker reduces communication signal component by exploiting leaky components or cross-modulation effects
Unauthorized Observation	Eavesdropping	An attacker listens to the crosstalk leaking from an adjacent signal through a shared resource in order to gain information from the adjacent signal

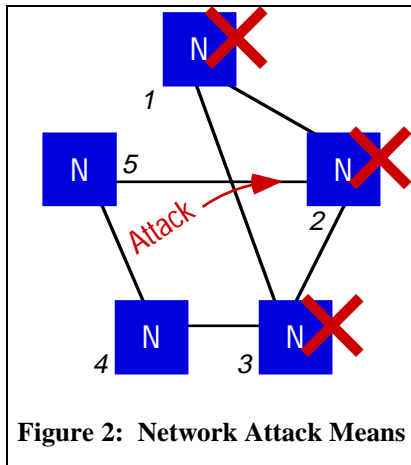
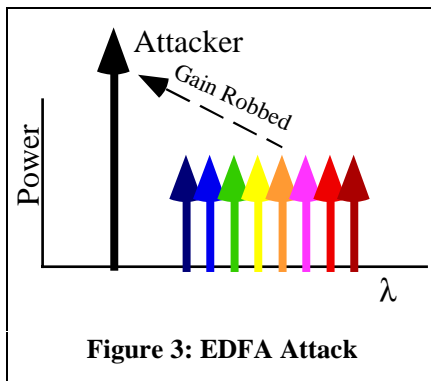


Figure 2 shows a single point attack on the center link (2,5), which affects not only the node which the attack signal first reaches (node #2), but the two other nodes with the first-attacked node connects (node #1 & node #3). The components from Table 1 that could be exploited are any of combiners, multiplexers, or optical amplifiers.

Single-point threshold in-band power detection would not necessarily suggest the correct location for the point of the attack. For instance, power detection at node #1 might wrongly ascribe the problem to an attack located at link (1,2). This attack can be made cheap, subtle, and can be specifically targeted at individual users.



A second attack is to employ *out-of-band jamming* to exploit crosstalk in optical components. Specifically, because of cross-gain modulation effects within an optical amplifier, jamming is possible by using an out-of-band high-power signal. This effect is very different from the gain compression effects found in electronic amplifiers. The attacker would inject a signal at a different wavelength from the communication bands, but within the amplifier passband, as shown in Figure 3. The attack can work because the amplifier cannot distinguish between attack signals and legitimate network

communication signals, and will provide gain to each signal indiscriminately from a finite supply of gain (specifically, its common wavelength-dependent gain-medium inversion). Those photons the amplifier provides to the attack signal both rob gain available to the communication signal, and increase the power of the attack signal downstream, allowing it to propagate through transparent nodes. Threshold in-band power detection at the receiver, the current accepted means of attack detection, would not necessarily detect jamming, because the average received in-band power could be made to decrease (not increase) or remain constant during the attack. This kind of attack could be mounted against an optical amplifier within a node or within an amplified fiber link.

EDFAs have different temporal behavior than conventional electronic amplifiers. The optical gain results from excitation of the erbium ions by absorption of a steady-state optical pump. The dynamics of the resulting excitation can be strongly affected by the signals being amplified particularly when they become intense enough to saturate the gain by extracting energy from the erbium excitation.

If the amplified signals vary rapidly compared to characteristic de-excitation times of the erbium ions (due to optical emission), then the erbium excitation varies with a slower time average of the optical signals. The gain is essentially constant as seen by the large-bandwidth signals being amplified. However, if there are long transients in the input signals or their envelopes, these transients can cause large transient changes in the erbium excitation, and the resulting gain. Even after the optical transients end, the gain changes may persist for much longer times (typically, 10's of microseconds or longer). This effect may provide a method for attacking an EDFA with an optical signal, in particular allowing a low duty cycle attack to be very effective at degrading or denying service.

The third attack is a realization of *unauthorized observation* (eavesdropping), the collection of signals by an attacker for whom they were not intended. Eavesdropping is possible at several points within the network — two examples are considered. The first example exploits component crosstalk — contemporary demultiplexers within network nodes exhibit crosstalk levels of between 0.03% to 1.0%. The demultiplexer is meant to separate each individual wavelength received from a single fiber onto separate physical paths, but the crosstalk allows a little of each wavelength to leak onto the wrong path. That signal may have enough fidelity to permit an attacker to detect its presence, and possibly to

recover a portion of the data from the stream. Within electronic or electro-optic regenerated networks, crosstalk levels are usually significantly lower than 0.03%, making eavesdropping via crosstalk less threatening. The second example exploits an optical amplifier. The gain provided by an EDFA to an individual channel is a function of the sum of the levels of all signals passing through the amplifier. This means that copropagating signals experience a slight amplitude modulation based on the presence or absence of signal on adjacent channels. An attacker can exploit that slight modulation to recover a portion of the intended signal on an adjacent channel. The optical amplifier attack can be effected in electro-optic, or all-optical networks.

3.4. Architectural Implications

Section 3.3 showed the vulnerability of some components — the individual methods of attacking portions of an AON infrastructure. When considering combination attacks and when analyzing attack detection algorithms, it is important to understand the broader impact of individual attacks upon the optical network architecture and services it provides.

Topology is an important architectural consideration, and different topologies have different security properties. Ring topologies allow attacks to be relatively easily localized, because of the structured interconnectivity of nodes. Rings also allow easy rerouting because there is only one logical link upon which traffic can be rerouted when an attack is detected. However, attacks on ring networks can generally require more work to restore services because all of the traffic on each ring is co-routed. The richer node interconnectivity of mesh topologies generally makes service restoration easier (though not in every comparison). However, the rich interconnectivity means that attacks aimed at transparent components are generally harder to detect. Star topologies make attack detection nominally easier than other topologies, because any propagating attacks are commonly received at many stations. However, compromise of the star network hub necessarily disrupts all network services. It should be clear from the foregoing that there is no one preferred topology to ensure the “best” network security, but also that the differences in vulnerabilities mean that each topology provides its own intrinsic security advantages. Most of the detection methods suggested in the following section will support any topology, though they’ll provide different defense levels based on the underlying topology and the type of network management system used. There has been work in the area of WDM AON network

management systems [15], [16], [17], [18]; further consideration of detection of attacks upon network management systems is beyond the scope of this paper. In general, the security services considered for higher layers of electronic packet networks [19] will not on their own be directly applicable to AONs. Some of these services will work well in conjunction with security systems operating at the physical layer.

4. Existing Methods for Attack Detection

4.1. A Categorization of Known Attack Detection Methods

This section examines the applicability of current automatic diagnostic and supervisory techniques to certain broad classes of attacks upon AONs. The supervisory techniques considered may be broadly arranged in two categories: (1) Methods which perform statistical analysis of the communications data (e.g. wideband power detection and optical spectrum analyzers); and (2) methods which measure a signal devoted to diagnostic purposes (e.g. pilot tones and optical time domain reflectometers).

Each is overviewed by type of attack and applicability for each of the three attack types described above.

4.1.1. Wideband Power Detection Methods

Power detection describes the measurement of received optical power over a wide bandwidth. It may be used to record a change in power with respect to the expected value. Because measured power is compared against an expected value, a slight decrease in power may take a long time to detect. If the law of large numbers is used in the statistical analysis, then a very long averaging time may be necessary to establish with reasonable certitude that a deviation of the sample mean from the statistical mean was statistically significant. Small but detectable changes in received power may not be attributable to attacks (e.g. component aging, fiber repairs, etc.) and may not adversely affect the communication signals. Therefore, most schemes use threshold power detection techniques with the selected thresholds matched to the level at which communication services will be degraded.

4.1.2. Optical Spectral Analysis Methods

Optical spectral analyzers (OSAs), as their name indicates, measure the spectrum of an optical signal.

There are many implementations of OSAs [20]. OSAs may give a more detailed diagnostic than simple power integration. They may be able to detect a change in spectrum shape, even if that change in shape does not entail a change in power over the whole channel. For instance, two signals can have the same total power but different spectra. An OSA will be able to distinguish between the two signals whereas a power integrator over the whole channel will not. Although OSAs may provide more information than power detectors, they still rely on statistical comparisons between sample averages and statistical averages. Arguments based on some law of large numbers will still imply that infrequent degradations of the signal will not be detected or will be detected only after a long time. Although providing more information than wideband power detection methods, optical spectral analysis methods generally require some averaging effects which make them slower than some other detection methods.

4.1.3. Pilot Tone Methods

Pilot tones are signals that travel along the same links and nodes as the communications data but which are distinguishable from that data. Their purpose is to detect transmission disruptions. Pilot tones are often at different carrier frequencies than the transmitted signal, but they might also be distinguished from the communications payload by certain time slots (in a TDMA system) or certain codes (in a CDMA system). Pilot signals are usually located at carrier frequencies within or between WDM channels as well as outside the transmission band. If the pilot tones are present, in frequency, in the close vicinity of the communications transmissions, they are usually referred to as subcarrier multiplexed (SCM) signals. Such SCM signals allow the transmission of network signaling or of a pilot tone at the same carrier wavelength as the payload signal [21]. The tone may be something other than a static tone. For instance, it may be dynamically tunable [22] to transmit network control information. The pilot tone may be at a lower frequency [23] than the communications signal or at a higher frequency [24].

The RACE project has adopted, as one of its diagnostic signals, a slow amplitude modulation of the high rate data communications signal. Such a modulation is a special case of an SCM pilot tone. There are some issues with interference between the data and the pilot tones. The experiments for the RACE project have indicated that the tone has negligible sensitivity degradation on a 622 Mbit/s NRZ pseudo-random data stream when the pilot frequency tone is below 100 KHz

and the tone amplitude is below 10 percent of the data level.

Cross-gain modulation among pilot tones at EDFAs has also shown that the pilot tone frequencies should remain between 10 and 100 kHz. Since these results were obtained by experimental testing, it is not clear how they apply to different data rates, modulation formats, etc. Moreover, there are issues associated with pilot tones traversing wavelength changers.

4.1.4. Optical Time Domain Reflectometry Methods

Optical time domain reflectometers (OTDRs) are a special application of pilot tones. Rather than analyze a pilot tone at the point where a communication signal is received, the pilot tone's echo is analyzed. Because of the widespread use of OTDRs and the fact that they analyze the reflection of the pilot tone rather than the pilot tone itself, OTDRs merit to be considered by themselves, although they share many features with pilot tones. OTDRs are generally used to diagnose faults, bends and losses in the fiber [25]. Thus, they would usually be better adapted to detecting attacks that involve fiber tampering. However, since they operate by reflecting a signal back through the fiber, they may also provide information about other attacks that are taking place. Note that the signal used for reflectometry may also be used as a supervisory signal [26], [27] and therefore may share the uses discussed in the section on pilot tones. The probe signal may also, for certain unmodulated or very simply modulated probe signals, be subject to jamming in the same way as pilot tones. Note that the use of optical isolators in conjunction with optical amplifiers is common, and may require OTDRs at every amplifier.

4.2. Existing Methods Applied to Defend Against an In-band Jamming Attack

4.2.1. Power Detection Methods

Power detection techniques are well suited to such problems as amplifier failures. They have been proposed as the basis of failure detection in AONs [28]. In the case of jamming, the power at the receiver would not be decreased but rather increased. A threshold detector could detect an overt jamming attack. A sporadic jammer may degrade the BER unacceptably without causing a strong enough rise in average received power to justify the generation of an alarm, particularly if the statistics of the received signal are not very tightly determined. Even if the statistics are tightly determined,

the sporadic nature of the attack may not cause statistical anomalies for a long time, while still affecting the very low BER that is required (typically 10^{-11} or less).

4.2.2. Optical Spectral Analysis Methods

An OSA will detect jamming attacks that significantly affect the received optical spectrum. Some of the uses of an OSA may be no different than the uses of a power detector, for instance if the OSA is used to detect a power surge due to a jammer. The OSA provides more information than that available from a wideband power detector but, for jamming through crosstalk, it may not provide much more information than a set of wavelength-specific power detectors. The main difference may be that the spectrum analyzer may show more information than a power detector and may therefore be more apt to detect changes in spectrum shape even when there is not sporadic or pulsed attacks.

4.2.3. Pilot Tone Methods

Pilot tones will not be effective in detecting jamming attacks unless those attacks cover the wavelengths at which the pilot tones are carried. Therefore, an attack at a certain wavelength may not affect a pilot tone at a different carrier wavelength. Thus, a broadband attack might be detected by pilot tones at different carrier wavelengths than the communication channels, but attacks that are bandlimited to the frequencies at which transmission of communications occurs, would not be detected. Even for SCM pilot tones, an attacker may be able to introduce a jamming signal, which disrupts communications without significantly affecting the SCM pilot signal. If the pilot signal is recovered through a bandlimiting filter approach, then an attacker need only remain outside the passband of that filter. Note that there are certain problems associated with filtering SCM signals. If the pilot tones are embedded in the frequency ranges where transmission occurs, there will be problems due to poor roll-off of the filters and to splitting the bandwidth assigned to a signal. Moreover, unless the pilot tones were hidden or dynamically hopped within the transmission band, the attacker would still be able to avoid the pilot tones when jamming by sending tones at different frequencies from the pilot tone.

The pilot signal may also be recovered by detecting it from its superposition with the communications signal. In that case, an attack upon the communications signal will have an effect upon the recovered pilot signal. The ability to detect an attack will depend upon the modulation and the SNR of the pilot tone. There are many examples of modulation of SCM signals [29]. In

the example of the RACE pilot tone, the low rate amplitude modulation may be considered as a very slow (with respect to the data rate) averaging. Therefore, if the communications system relies on low data BER, the communications signal may be significantly affected without affecting the detection of the pilot tone. For instance, if 1 percent of the 0s are mapped to 1s by the introduction of a spurious signal, then a 50 kHz pilot tone is unlikely to be affected. If, moreover, the jamming signal has the same slow amplitude modulation as the legitimate communications signal, which may be tracked if it is sufficiently low frequency, then the introduction of the jamming signal may not affect the recovery of the pilot signal. Therefore SCM pilot tones offer more protection against jamming than pilot signals on different wavelengths but still allow a range of jamming attacks, which may be very detrimental to the communications signals. Note that pilot signals may be subject to jamming themselves. Suppose that a pilot tone is not modulated or is modulated in such a way that a user can inject a signal, for instance via crosstalk, which will introduce a spurious pilot tone. In that case, raising the SNR of the detected pilot tone by addition of a spurious signal may mask jamming attacks.

4.2.4. Optical Time Domain Reflectometry Methods

If there is a wideband jamming attack, then some of the jamming signal will be returned in the reflections and should be observable. Such a diagnostic differs from that offered by a pilot tone in that the diagnostic may be done at the head-end. If there is some modulation on the OTDR probe signal [30], then detection of a jamming signal superimposed on the OTDR probe signal may be fairly sensitive. In branched networks, such as networks where wavelengths are demultiplexed onto different fibers, different branches may be individually probed by sending different wavelength probe signals [31]. Therefore, jamming may be detected over different branches and its spreading through a branched network may be traced. A different technique uses filtering of the ASE by different fiber Bragg gratings (FBGs) on each branch to generate a probe signal [32]. Such a technique would not be able to detect jamming if the addition of the jamming signal were to occur before the FBGs.

4.3. Existing Methods Applied to Defend Against an Out-of-Band Jamming Attack

4.3.1. Power Detection Methods

In the case of gain competition, the received signal power may be decreased. However, certain gain competition attacks may lead to a severe degradation in SNR without degradation in total power. Suppose that a signal "s" must traverse two EDFAs, A_1 and A_2 . If there is gain competition at A_1 , the signal s may not be adequately amplified. At A_2 , the signal received will have proportionally more ASE from A_1 than if there had been no gain competition. With some automatic gain control (AGC - a method which maintains A_2 's output power at a specified level), at A_2 , the signal received after A_2 may consist disproportionately of ASE from A_1 superimposed upon ASE from A_2 . Note that if the gain of A_2 were fixed (no AGC), the signal output from A_2 would be lower in power than if there had been no gain competition at A_1 .

Another attack combines gain competition with jamming to thwart power detection techniques. For this technique to be effective, it does not matter whether or not A_2 has automatic gain control. The amplifier A_1 , located before a point of crosstalk jamming such as a switching fabric, is subject to gain competition. The insertion of a jamming signal through crosstalk after A_1 replaces the power of the legitimate signal s lost to gain competition. Thus, the power at the input of A_2 would be as expected by the network and A_2 would amplify a weak version of s superimposed with a jamming signal and ASE from A_1 . Such a gain competition followed by jamming scenario can occur if A_1 is a pre-amp in front of a switching fabric, which exhibits crosstalk. Thus, power detection techniques may not be satisfactory.

4.3.2. Optical Spectral Analysis Methods

OSAs may be of use to determine the source of a gain competition attack, as long as the band that is analyzed by the OSA is sufficiently large to encompass the carrier frequency of an out-of-band attack. A particularly nefarious attack can occur if the attacker introduces a signal in the most peaked area of the gain spectrum. An OSA may be able to show the presence of such an out-of-band attacker even though power detection on the individual channels will not.

4.3.3. Pilot Tone Methods

Gain competition affects all wavelengths through an amplifier, although not all wavelengths are equally affected and there is dependence upon the saturating wavelength. If the pilot signals traverse the same amplifiers as the communication signals, then the pilot signals should be affected by gain competition when the communication signals are. If the pilot signals are amplified separately, then they will not enable detection of a gain competition attack.

Even if the pilot tones are amplified in the same amplifiers as the communication channels, the pilot tones may, under certain conditions, not be of use in detecting gain competition attacks. For a tone, detectability requires a much lower SNR than that required to obtain adequate BER on a communication link. Therefore, the methods used to detect the presence of a pilot tone, for instance to detect a fiber cut, may not be as sensitive to degradation as the methods used to detect a communications signal. In particular, if there is AGC, then the total power in the band of the pilot tone may be sufficient to mask the occurrence of gain competition. Let us suppose that a pilot tone suffers from gain competition at amplifier A_1 . If it then passes through amplifier A_2 with AGC, then the total power received for the pilot tone signal may be unaffected but the communication signal, as described in the previous section on power detection may be corrupted by ASE. Even if the modulation and detection of the pilot tone is done in such a manner as to allow detection of attacks which may disrupt communications, certain gain competition attacks may be able to overcome detection by a pilot tone. The attack is the same as the one described for the power detection case. The gain competition/jamming combined attack could be used to thwart attempts at detecting gain competition through observation of the pilot tone. If the modulation of the pilot tone is known, then for certain modulations a jammer may introduce a spurious pilot tone via crosstalk after the occurrence of a gain competition attack.

4.3.4. Optical Time Domain Reflectometry Methods

The probing of EDFAs by OTDRs is not similar to the probing of fiber lines by OTDRs. If the EDFAs are unidirectional, then they are not useful for amplifying reflected signals and a bi-directional amplifier is required. Therefore, OTDRs will not generally be useful in determining gain competition among signals over a cascade of EDFAs. If an EDFA is used as a preamplifier for the OTDR as well as a power amplifier for the communications system, then gain competition at that

EDFA should be detectable over the reflected OTDR probe. The EDFA probe signal, for the purpose of gain competition detection, then fulfills the same purpose as a pilot tone. The probe signal may be jammed with noise or by insertion of a spurious probe signal, with the same class of attacks that may be levied against a pilot signal. Note that there are certain filtering issues that arise from the use of in-line EDFAs as pre-amplifiers for OTDRs [33].

4.4. Existing Methods Applied to Defend Against a Tapping Attack

4.4.1. Power Detection Methods

Power detection techniques have been applied to detection of tapping by detecting the loss of power [34]. In [35], the modulation is constrained to on-off keying with a small modulation index. In [36], the modulation is frequency shift keying. The basis of these types of security systems is that only an eavesdropper who drains a significant amount of power can perform satisfactory detection of such a signal. A drain of power sufficiently large to enable an eavesdropper to detect adequately through tapping is noticed by an attack detection system. There are many drawbacks to this scheme. It is modulation specific, since it is predicated on on-off keying or frequency shift keying. Moreover, by restricting consideration to modulations with a very small modulation index, the legitimate user's available data rate is significantly reduced. Finally, the system is not robust to an attack where a jamming signal is inserted after the tapping point. Indeed, a power detection mechanism would consider the jamming noise as part of a legitimate untampered signal. In general, power detection methods for tapping will not be adequate on the tapped channel if (1) Tapping does not reduce the received power sufficiently to trigger an alarm, for instance because the tap is sporadic and very short or because the tap drains a very small portion of the legitimate user's power, or (2) Tapping at the fiber is followed by the insertion of a spurious signal to raise the total received power.

Observing the power at the tapping channel through the fiber crosstalk may enable the attack detection mechanism to detect an increase in power due to the presence of the tapped signal. Without any means of verifying the source of the added power, however, it may be difficult to determine whether the extra power arises from greater transmitter power, increased amplification, benign effects of crosstalk, etc., or from an attacker.

4.4.2. Optical Spectral Analysis Methods

OSAs will not be able to detect eavesdropping on the channel that is tapped unless the eavesdropping leads to a disruption of the tapped signal, e.g. a drop in channel power or a change in spectrum which is greater than that which is allowable under normal operating conditions. Thus, eavesdropping through crosstalk should not cause an OSA analyzing the tapped signal to detect any significant changes. However, as in our discussion of other detection means, OSAs may be able to detect tapping by observing changes on the tapping channel. For the OSA to be useful in detecting changes in the tapping channel, there must be some means to determine that the communication present on the tapping channel is not legitimate. Such determination is difficult unless the communications are easily identifiable. For instance, using the outputs of several OSAs to compare them for possible tapping of one channel by another is onerous and difficult.

4.4.3. Pilot Tone Methods

If pilot tones are detected only for the communications that are supposed to be received, as is the case in current systems, then they can provide no protection against eavesdropping. Unless the act of tapping the communication channel (fiber) causes significant degradation of the signal, then the pilot tone on the tapped channel would not be affected.

4.4.4. Optical Time Domain Reflectometry Methods

OTDRs may be used to detect in-line eavesdropping, which requires some tampering with the fiber. The OTDR will detect discontinuities or losses in the fiber due to the extraction of a portion of the signal for eavesdropping. However, as for pilot tones, eavesdropping which occurs through crosstalk that is legitimately present in the network cannot be reliably detected without a search for traces of OTDR probe signals on fibers which may be carrying communications tapped from other fibers.

4.5. Summary

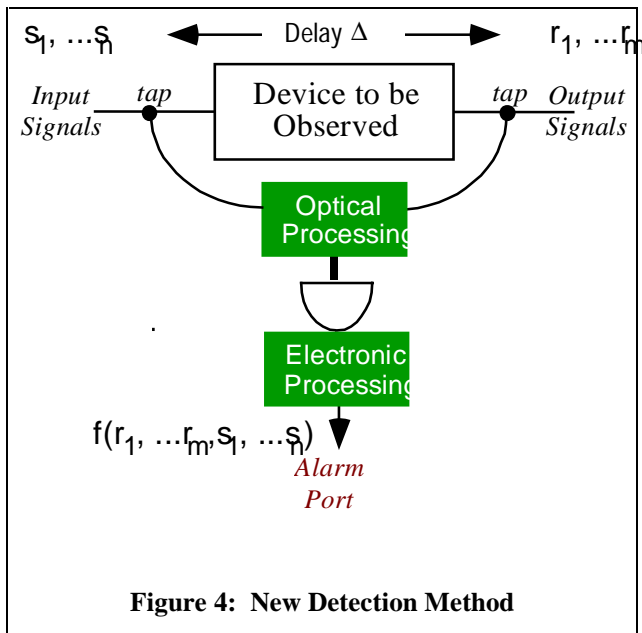
This section has detailed four methods that might be applied to the attack detection problem for AONs: wideband power detection, optical spectral analysis, pilot tones, and time domain reflectometry. Each has strengths and weaknesses with respect to an individual network architecture and attack methods, and none can provide protection against each attack method considered. Particular strengths include the detection of

single-location overt jammers by pilot tones, power detectors, and OSAs, as well as the possibility of OTDRs to detect certain eavesdropping attacks. Limitations include the fact that power detection and OSA techniques are susceptible to sporadic attacks, and pilot tone and OTDR techniques do not protect against eavesdropping.

5. A New Method for Detecting Attacks Upon All-Optical Networks

This section describes a new method for detecting attacks at optical nodes and within amplified links in transparent AONs. Transparent networks do not afford a single integrity test on either the input or the output of any device within the network. Except for simple tests (e.g. total power, the limitations of which were explored in section 4), no quantitative test can be used for attack detection since the legitimate signal could be modulated in any way. However, consideration of device input and output together even for a transparent network can yield a reasonable test. The new method is based on the notion that the input and output signals of a device should have a mathematical relationship that is well known by the network management system that provisions the service. Therefore, a comparison of the input and output signals might be able to detect an attack if the some function of the signals does not conform to an a priori known set of parameters.

The general case is shown in Figure 4. Multiple input signals (s_1, \dots, s_n) enter the device from the left, and exit as output signals (r_1, \dots, r_n) at the right. The observed device could be an optical amplifier within a fiber link or node, a demultiplexer/switch/multiplexer within a node, or a star-combiner in a local-area network hub (or other combinations of devices from Table 1). The detection method inserts a tap into both input and output signal paths, and splits off a known, but negligible portion of the signal for testing. A delay matching the intrinsic delay of the observed device is added to the signal from the input path tap. The input and output path taps are fed to an optional optical processing unit. Both tapped paths are then photodetected, and the result is an electrical signal that is processed in the electronic processing unit, whose output is $f(r_1, \dots, r_n, s_1, \dots, s_n)$. The processing attempts to detect the presence of an attack. The function f measures the operation of the device with respect to some nominal parameters. The value of f determines whether or not an alarm is generated. Note that this technique does not require changing the observed device in any way, rather it forms a *wrapper* around the device. It also decouples (to some extent) the security protection afforded a device from the design and manufacturing of the devices itself. The alarm port is assumed to be connected to a network management system that can process the alarms from all observed network devices. The remainder of this section presents examples of particular implementations of the scheme sketched in Figure 4.



5.1. Amplitude Comparison

One of the simplest forms of the idea is shown in Figure 5. The idea is to photodetect the signal at the input and output ports of the observed device. Photodetection is a square-law detection process. The difference between the two photodetector outputs, possibly adjusted for gain, is therefore the difference in amplitude of the input and output signal. That difference is compared against an estimate of what the difference should be under nominal operation of the device, thus giving an indication of an attacker's presence. This scheme is a short time scale approach (e.g. bit-by-bit) to determine whether an alarm should be generated. It is intrinsically different from a statistical test (e.g. power averaging) that were described in section 4.4.1.

As an example, consider the output of the two detectors where the observed device is an optical amplifier. The input and output should differ only by a multiplicative factor – the amplifier gain (amplifier noise is added during amplification, but for the moment it is ignored). Therefore, assuming the delay Δ is matched to the amplifier transmission path, and that the gain in the amplifier following the output photodetector is set to the inverse of the gain of the observed device, the difference between the two arms should be zero under normal operation. If an attacker challenges the amplifier with out-of-band jamming, the arms would become unbalanced and the threshold would be exceeded, generating an alarm. A very important observation is that the scheme does not depend upon the data rate or modulation format of the data passing through the observed device. The scheme does require careful matching of the path delays to ensure comparison of the same section of signal. The exact requirements for matching are dependent upon the traffics flowing through the transparent network.

The scheme will guard against attacks that affect the amplitude of a signal but it provides no information about the phase. Thus, for certain types of modulations such as phase shift keying, this method would be unable to detect phase only attacks. This scheme will also not guard against the possibility that the attacker has direct physical access to the monitor ports - we are in effect assuming that all nodes all repeater/regenerator locations and security wrappers are enclosed within their own secure enclaves. The analysis does not require that the long haul installed fiber plant be secure, nor does it require that each terminal location be within a secure

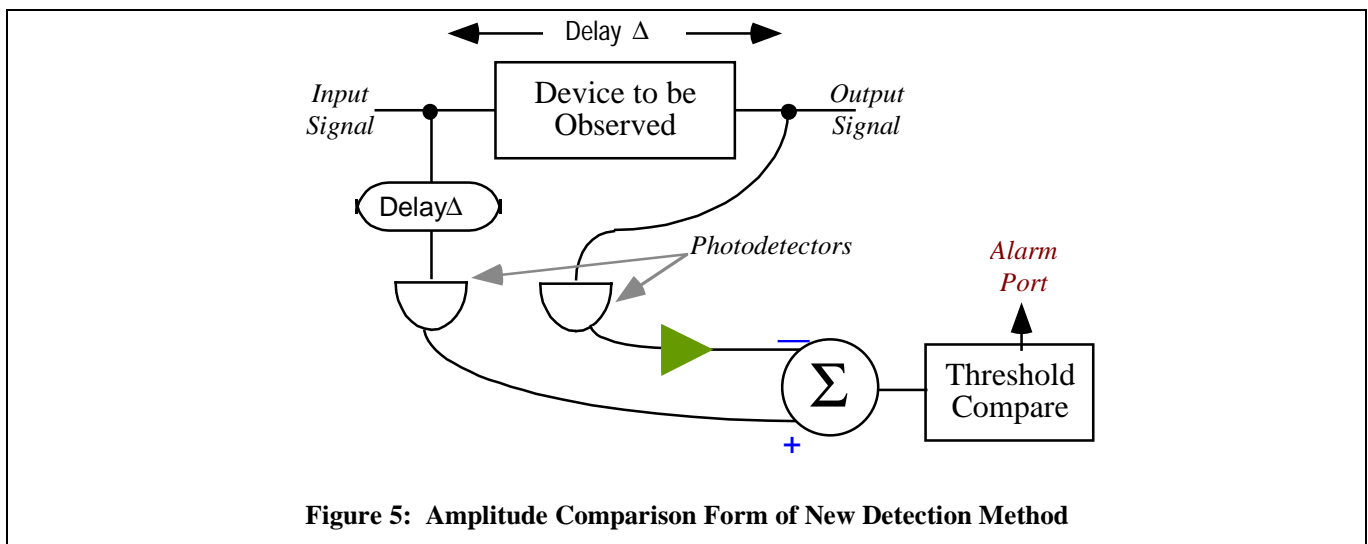
enclave. The scheme will effectively guard against attacks sourced from the long haul fiber plant, outside secured nodes.

5.2. Phase and Amplitude Comparison

A more sophisticated means to detect attacks is outlined in Figure 6. Instead of directly photodetecting the input and output of the observed device, the outputs are first optically processed to produce the sample correlation of the input and output signals using an optical delay-and-sum operation. The advantage over the previous method is that a class of attacks that affect amplitude and/or phase will be detected, although certain combined phase and amplitude attacks will not be detected. The principal disadvantage is that the amplitude and phase comparator requires more hardware than the amplitude comparator.

5.3. Important Detection Issues

Though a comprehensive analysis of the detection scheme is beyond the scope of this paper, some performance related issues merit mentioning. Of particular interest are (1) the detection time necessary to ferret an attacker, (2) the likelihood that an alarm is generated when no attacker is present (false positive case), and (3) the likelihood that an attacker eludes the detection mechanism while successfully attacking the network (false negative case). These three problems are mathematically linked.



The detection time for this method is dependent upon the optical power received at the photodetectors and the threshold used for the comparison. It is not dependent upon the number of bits received. Because of the dependence upon optical power, there is a tradeoff among the signal-to-noise ratio (SNR) of the signals on the fiber (and the loss in the observed device), the detection time, and the degree of certitude desired to assert an attack is underway.

False positives and false negatives are metrics that are interwoven by a single threshold selected in the comparator in the electronic processing section. Both false positive and false negative results are dependent upon the SNR, the detection time allowed, the noise levels in the observed device. For a single tone in-band jammer having the same relative power as the communication signals themselves, false positive and false negative values can be achieved on the order of the bit-error-rate of the communication signal.

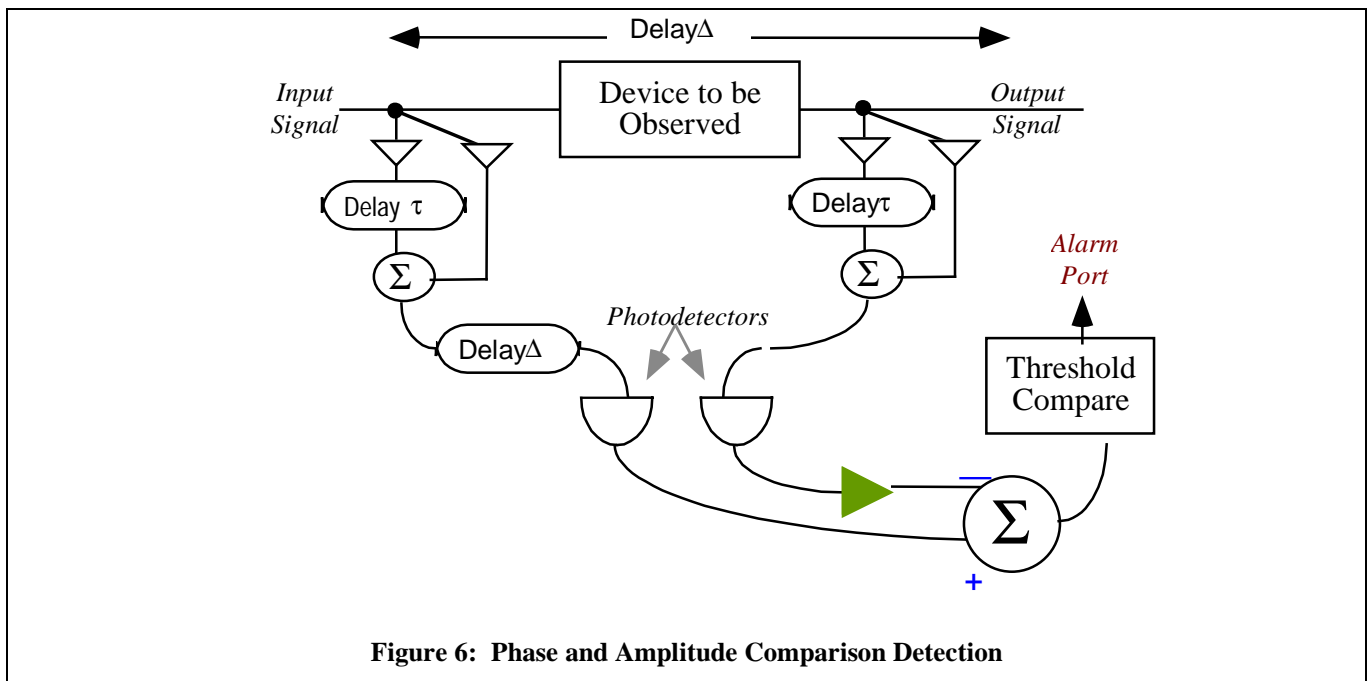
5.4. Impact

It is reasonable to question the system effectiveness of such a detection scheme. The most obvious means of determining attacks upon a digital communication link is to monitor bit error rate, and generate an alarm when the number of bit errors in a specified interval exceeds a threshold value. For example, in a SONET link with an approximate 10^{-11} bit error rate, and assuming a 1 Gbit/s communication link with 20 dB SNR, one means of deciding that an attack is underway is to set a BER

threshold at a value higher than the nominal, for this example 10^{-8} is chosen. For this assumption, detection of the attack would require times on the order of hundreds of milliseconds to seconds depending upon the confidence required. In contrast, the scheme shown in Figure 6 would require on the order of hundreds of nanoseconds to microseconds for the same detection probability, an improvement of about six orders of magnitude. This improvement gives some confidence that further development and analysis of similar algorithms and schemes may well provide the advanced level of attack detection necessary for tomorrow's secure optical networks. This method may be useful in detecting a lost quality of service even during sporadic attacks.

6. Discussion and Concluding Remarks

This final section contains a brief review and discussion of the limitations of the detection means considered. Section 2 provided an overview of AONs. Section 3 outlined a set of infrastructure vulnerabilities in AONs that differ in some way from the vulnerabilities in electronic or electro-optic networks. Section 4 reviewed the possible application of four existing detection and diagnostic methods to the problem of detecting attacks of the type discussed in section 3. While each of the four methods reviewed can detect certain classes of attacks, none can provide protection against more than one class of fairly simple attacks. Section 5 discussed a new mechanism for attack



detection that is applicable to amplified links and optical network nodes, and gave two examples of possible realizations. The ability to protect unmodified existing devices via a wrapper technique is desirable.

While it is possible to provide continually more advanced means to detect attackers, both technical ability and security budgets will limit what is ultimately installed in an infrastructure. The most important challenges include:

- **Sporadic Jamming**, which attempts to disrupt service but “disappear” before it can be detected. Cryptography will solve part of the problem, but faster attack detection and multipath routing could provide more significant defenses.
- **Multipoint Attacks**, which attempt to thwart service and to avoid detection methods that attempt to localize them. These attacks are potentially much more pernicious if the attackers are well synchronized. Advanced algorithms for network management systems are one means of increasing defenses against such serious attacks.
- **Control System and Protocol Attacks**, which attempt to confuse the network controlling mechanisms into believing failures exist, usually to provoke reactions that negatively affect the network services. Sporadic jamming combined with a protocol attack can become even more problematic if cleartext headers are exploitable by an attacker.

The new detection scheme presented provides some defenses against sporadic jamming, and some defenses against multipoint attacks assuming an advanced algorithm running in a network management system. This work has not yet considered control or protocol attacks. Future work should include appropriate reaction method (e.g. rerouting).

The most compelling economic limitation encountered may be the cost of retrofitting an inherently insecure infrastructure to make it more secure. While the methods and means to secure the infrastructure proposed herein are not free, their relatively simple implementation, and lack of requirement to change existing AON devices, may make these security measures far less expensive than field retrofitting of nodes and links.

7. Acknowledgement

We acknowledge Poompat Saengudomlert's contribution to the analysis on the new attack detection mechanism.

References

-
- [1] M. Médard, D. Marquis, R.A. Barry, S.G. Finn, “Security Issues in All-Optical Networks”, IEEE Network Magazine, May 1997.
 - [2] D. Marquis, M. Médard, S. G. Finn, R. A. Barry, “Physical Security Considerations in All-Optical Networks”, SPIE Proceedings, November 1997, Dallas, Texas.
 - [3] R.A. Barry et al., “All Optical Network Consortium – Ultrafast TDM Networks”, IEEE Journal on Selected Areas in Communications, vol. 14, no. 5, June 1996, pp 999-1013.
 - [4] <http://www.ll.mit.edu/aon/>
 - [5] C.A. Brackett et al., “A Scaleable Multiwavelength Multihop Optical Network: A Proposal for Research on All-Optical Networks”, Journal of Lightwave Technology, vol. 11, no 5/6, June 1993, pp 739.
 - [6] <http://www.ntonc.org/>
 - [7] G.R. Hill, P.J. Chidgey, F. Kaufold, T. Lynch, O. Sahlen, M. Gustavsson, M. Janson, B. Lagerstron, G. Grasso, F. Meli, S. Johansson, J. Ingers, L. Fernandez, S. Rotolo, A. Antonielli, S. Tebaldini, E. Vezzoni, R. Caddedu, N. Caponio, F. Testa, A. Scavennec, M.J. O'Mahony, J. Zhou, A. Yu, W. Sohler, U. Rust, H. Herrmann, "A Transport Network Layer Based on Optical Network Elements", Journal of Lightwave Technology, vol. 11, no. 5/6, May/June 1993, pp.667-679.
 - [8] H. Onaka et al., “1.1 Tb/s WDM Transmission over a 150 km 1.3 nm Zero Dispersion Single-Mode Fiber”, Proc. Opt Fiber Conf. (OFC '96), San Jose, Ca, Feb 1996, Postdeadline paper PD19
 - [9] B. R. Hemenway et al., "Demonstration of a Reconfigurable Wavelength Routed Network at 1.14 Tbit/s", OFC 97 Postdeadline Paper PD-26, February 1997.
 - [10] R.L. Hughes et al., “Quantum Cryptography”, *Contemporary Physics*, vol. 36, no. 149, 1995.
 - [11] A.H. Chan, M. Médard, “Reconfigurable Feedback Shift Registers”, *Proceedings of the 1997 International Symposium on Information Theory*, pg. 178

-
- [12] M. Médard, A. H. Chan, J. D. Moores, K. A. Hall, K. A. Rauschenbach, S. A. Parikh, "Ultrafast Cryptography Using Optical Logic in Reconfigurable Feedback Shift Registers", SPIE Proceedings, November 1997, Dallas, Texas.
 - [13] W. R. Cheswick, S. M. Bellovin, "Firewalls and Internet Security", Addison-Wesley, 1994, ISBN 0-201-63357-4
 - [14] I. Katzela, G. Ellinas, T.E. Stern, "Fault Diagnosis in the Linear Lightwave Network", LEOS Summer Topical Meetings, August 7-11, 1995, pp.41-42.
 - [15] M.W. Maeda, "Management of WDM Optical Networks", Optical Fiber Communication Conference 1997 tutorial, February 1997, pp. 141-166.
 - [16] "IEEE/COMSOC Workshop on WDM Network Management and Control", June 23, 1996, Dallas, Texas.
 - [17] M. Bischoff, M. H. Huber, O. Jahreis, S.A.F. Derr, F. Ulm, "Operation and Maintenance for an All Optical Transport Network", IEEE Communications Magazine, November 1996, pp. 136-142.
 - [18] C.-S. Li, R. Ramaswami, "Automatic Fault Detection, Isolation and Recovery in Transparent All-Optical networks", Journal of Lightwave Technology, October 1997, vol 15, no 10, pp 1784-1793.
 - [19] B. Schneier, "Applied cryptography : protocols, algorithms, ...", Wiley, New York, 1994, ISBN:0471597562
 - [20] L.F. Stokes, D. Derickson, "Lightwave Component and System Measurements", Short Course Notes, OFC 97.
 - [21] C.-L. Lu, D.J.M. Sabido IX, Perluigi Poggioni, R.T. Hofmeister, L.G. Kazovsky, "CORD- A WDMA Optical Network: Subcarrier-Based Signaling and Control Scheme", IEEE Photonics Technology Letters, vol. 7, no. 5, May 1995, pp.~555--557.
 - [22] B.H. Wang, K.Y. Yen, W.I Way, "Demonstration of gigabit WDMA systems using parallel processed subcarrier pilot-tone signaling technique", in OFC'96, paper TuE1.
 - [23] A. Kloch, B. Mikkelsen, K.E. Stubkjaer, "Pilot tones in WDM networks with wavelength converters", OFC, 1997, TuE6
 - [24] M.J. Minardi, M.A. Ingram, "Adaptive Crosstalk Cancellation and Laser Frequency Drift Compensation in Dense WDM Networks", Journal of Lightwave Technology, vol. 13, no. 8, August 1995, pp.~1624--1635
 - [25] Guide to OTDR Measurements, Anritsu Wiltron, 1995.
 - [26] Y.W. Lai, Y.K. Chen, W.I. Way, "Novel Supervisory Technique Using Wavelength-Division-Multiplexed OTDR in EDFA Repeated Transmission Systems", IEEE Photonics Technology Letters, vol. 6, no. 3, March 1994, pp.446-451.
 - [27] Y.-K. Chen. S. Chi, "Fault-Locating and Supervisory Technique for Multistaged Branched Optical Networks", IEEE Photonics Technology Letters, vol. 6, no. 7, July 1994
 - [28] N. Schroff, M. Schwartz, "Fault Detection/Identification in the Linear Lightwave Network", CU/CTR/TR 243-91-24, Columbia University, 1991
 - [29] S. Betti, E. Bravi, M. Giaconi, "Analysis of Distortion Effects in Subcarrier-Multiplexed (SCM) Externally Modulated Systems: A Generalized Approach", IEEE Photonics Technology Letters, vol. 9, no. 1, January 1997, pp.118-120
 - [30] M. Sumida, "OTDR Performance Enhancement Using a Quaternary FSK Modulated Probe and Coherent Detection", IEEE Photonics Technology Letters, vol. 7, no. 3, March 1995, pp.336-338.
 - [31] F. Yamamoto, I. Sankawa, S. Furukawa, Y. Koyamada, N. Takato, "In-service Remote Access and Measurement Methods for Passive Double Star Networks", Conference on Optical Hybrid Access Networks, pp.5.02.01-06
 - [32] C.-K. Chan, F. Tong, L.-K. Chen, J. Song, D. Lam, "A Practical Passive Surveillance Scheme for Optically Amplified Passive Branched Optical Networks", IEEE Photonics Technology Letters, vol. 9, no. 4, April 1997, pp.526-528
 - [33] W.I. Way, Y.W. Lai, Y.K. Chen, "The Effect of Transient Gain Compression in a Saturated EDFA on Optical Time Domain Reflectometry Testing", IEEE Photonics Technology Letters, vol. 6, no. 10, October 1994, pp.1200-1202
 - [34] A.V. Yakovlev, "An Optical-Fiber System for Transmitting Confidential Information", Telecommunications and Radio Engineering, (4), 1995. pp.~1--6
 - [35] R. Erkander, "Optical Fibre Security System ZAT 4", Ericsson Review, Vol. 67, no. 1, 1986, pp.35-41.
 - [36] J.H. Bowen, D.L. Baldwin, P.R. Couch, "Secure Fiber Optic Data Transmission System", United States Patent no. 4,435,850, March, 1984.